IN THE U.S. PATENT AND TRADEMARK OFFICE

#16 Brief

Appl. No.	:	09/559,499
Applicant	:	Piikivi et al.
Filed	:	April 27, 2000
TC/AU	:	3625
Examiner	:	Yogesh C. Garg
Docket No.	:	872.0017.USU
Customer No.	:	29683

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S APPEAL BRIEF

Sir:

Commensurate with the NOTICE OF APPEAL filed on August 15th, 2003 (and mailed on August 13th, 2003), Applicant/Appellant hereby submits this APPEAL BRIEF to the Board of Patent Appeals and Interferences (hereinafter, the Board) under 37 C.F.R. 1.192 and M.P.E.P. § 1206 in triplicate, and a draft for the $330 appeal brief fee set forth in 37 C.F.R. 1.17(c). This BRIEF is filed within two months from the filing date of the above-cited NOTICE and the undersigned representative believes that no late fee is due. However, should the undersigned attorney be mistaken, please consider this a petition for an extension of time under 37 C.F.R. § 1.136(a) or (b) that may be required to avoid dismissal of this appeal, and debit Deposit Account No. 50-1924 as appropriate.

(1) REAL PARTY IN INTEREST

The real party in interest (RPI) is the Nokia Corporation of Espoo, Finland. This invention was assigned to Nokia Mobile Phones Limited, which at the time of assignment was a

wholly owned subsidiary of Nokia Corp. Nokia Mobile Phones Limited is no longer a separate business entity, and its assets, including the present invention, have become the property of Nokia Corp.

(2) RELATED APPEALS AND INTERFERENCES

There are no other pending appeals or interferences of which the undersigned representative and assignee/RPI is aware that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

(3) STATUS OF CLAIMS

Claims 1, 3-7, 9-16 and 18-31 are pending in this appeal, and are reproduced in an Appendix accompanying this Brief as those claims stood finally rejected by an Office Action dated July 16, 2003, with the exception that claim 31 reflects a correction to a typographical error noted below. Claims 1-20 were originally filed with this application, and claims 3, 6, 10-15, and 18-20 remain unchanged.

In response to an Office Action dated July 3, 2002, claims 1, 5, 7, 9 and 16 were amended and claims 21-32 were added. In response to an Office Action dated November 8, 2002, claims 1 and 5 were again amended. In response to an Office Action dated March 6th, 2003, claims 1, 7 and 16 were again amended, claim 31 was amended for the first time, and claims 2, 8, 17, and 32 were cancelled. The Notice of Appeal dated August 15th, 2003, corrected a typographical error in claim 31, which was acknowledged by the Examiner in an Advisory Action dated September 24th, 2003.

(4) STATUS OF AMENDMENTS

With the exception of the correction to the typographical error in claim 31 noted immediately above, no amendment to the claims was proposed subsequent to the Final Rejection dated July 16th, 2003.

(5) SUMMARY OF INVENTION

The present invention is in the context of a user communicating with a server or an internet site such as a commerce-related site on the world wide web (for brevity, hereinafter referred to as a website) using both a computer and a wireless mobile station such as a cellular telephone. Embodiments of the invention detailed in the claims include communication methods, a communication system that includes a mobile station and a computer, and the mobile station.

It is common practice for a user to access websites using a computer. When the user seeks to purchase a product or service from the website, the website sends a message requesting payment, to which the user responds with a credit card number, digital signature, private encryption key, authorization certificate, or other payment information. Certain computers may be accessible by more than one individual, so individual users may choose not to store credit card information in the computer itself.

To eliminate the need for the user to retrieve and reference a credit card number or other un-memorized payment information that may be frequently re-used, the present invention adds to the above transaction a mobile station that is wirelessly connected to the computer. The un-memorized payment information may be stored in the mobile station. The

computer automatically passes to the mobile station a request over a wireless link in response to receiving a request from the website. The mobile station receives the request, prompts the user to enter a personal identification number (PIN), compares the PIN to that stored in the mobile station, and responds through the computer and the wireless link to the website's request.

Certain claims broaden the above website to be any data communications network (claims 7, 9 and 16), or the communication to be with a server (claim 31). Other claims apply to various messages the website may send and various replies that the mobile station may return, which in certain claims includes user authentication or identification. Claim 22 addresses an embodiment wherein the message is a challenge that is detected by message parsing; claims 23 and 31 address an embodiment wherein the website sends a request, the computer in response sends an inquiry to the mobile station for an applicable certificate, the mobile station presents the user with a list of applicable certificates, and the mobile station passes a completed certificate to the computer, which then provides the completed certificate to the website. Claim 30 is directed to a mobile station that presents the user with a list of certificates. Further implementation details, such as using a browser, using an access application, an authentication module, etc., are recited in various independent and dependent claims.

(6) ISSUES

A. The first issue presented for review by the Board is whether any combination of references teaches or suggests a limitation found in each of the independent claims 1, 7, 16, 22-23, or 30-31, namely, that a computer automatically sends a message to a mobile

station in response to receiving a particular message from a commerce-related site or server. The references include U.S. Patent No. 6,175,922 B1 to Wang (hereinafter, Wang), U.S. Patent No. 6,269,336 to Ladd et al. (hereinafter, Ladd), and U.S. Patent No. 6,256,664 B1 to Donoho et al. (hereinafter, Donoho). Dependent claims 11-12, 18 and 21 are also argues in the context of the first issue.

B. The second issue is whether the Wang reference anticipates, under 35 U.S.C. § 102(e), a list of certificates as recited in each of claims 23-25 and 28-31.

C. The third issue is whether the Wang reference can be modified to make obvious that a user authentication message or user personal identification is passed outside a mobile station as recited in claims 1, 10 and 28.

(7) GROUPING OF CLAIMS

All claims form a first group in which a first clause common to all claims is argued under Issue A as not being anticipated, taught or suggested by Wang (as suggested by the Examiner) or any of the cited references.

Claims 23-25 and 28-31 form a second group, in which a second clause common to each of them is argued under Issue B as not anticipated by Wang. The second group may stand together with but do not fall with other claims from the first group, as the second clause is contended independent grounds for patentability.

Claims 1, 10 and 28 form a third group, in which a third clause is argued under Issue C as not within Wang and not an obvious modification of Wang. The third group may stand together with but do not fall with other claims from the first or second group, as the third clause is contended independent grounds for patentability. Additionally, claim 28 stands or falls independently of claims 1 and 10, as the argued limitation is implied in claim 28 and explicit in claims 1 and 10.

(8) ARGUMENT

Issue A: Does any combination of references teach or suggest a computer automatically sending a message to a mobile station in response to receiving a particular message from a commerce-related site or server?

Claim 1 recites in relevant part:

> in response to automatically detecting the presence of the message, sending a message from the computer to a mobile station over a bi-directional transmission link;

Each and every pending independent claim recites, in language that may vary slightly between claims, that a message be automatically sent to the mobile station when a particular message from a website is detected. This clause reflects an amendment dated September 9, 2002, that was made in response to a 102(e) rejection over Wang. In the final Office Action dated July 16, 2003, the Examiner cited only Wang as teaching this aspect of the claimed invention.

Wang is directed to a method and portable electronic authorization device (PEAD) for authorizing electronic transactions. The methods of Wang include receiving an executable portion of a program at a computer or ATM, using the executable portion to search for the PEAD, approving the transaction at the PEAD, and transmitting the approval from the PEAD. See Wang, col. 3, lines 8-20, 24-35 and 39-55. In the terminology of Wang at col. 4, lines 56-61 and col. 5, lines 38-39, the requesting device 202 is an ATM, computer, network, etc. that permits a user to transact business with an electronic transaction system, of which the requesting device is a part.

Wang details a transaction program (TP) downloaded from a server 902 to the requesting device 202 at col. 14, line 63, et seq. Wang describes that the executable portion of the TP may automatically detect the presence of the PEAD (col. 16, lines 7-10), and that the TP may communicate with the PEAD after detection (col. 16, lines 52-54). However, Wang does not appear to disclose that the requesting device automatically send a message to the PEAD in response to receiving the TP.

The Examiner recites at page 11 of the Office Action dated July 16, 2003, that Wang impliedly teaches this automatic aspect, and that such an implied teaching is in line with the rationale recited in the present patent application. The Examiner cited two portions of the application as providing rationale for that supposed implied teaching, each portion describing the present invention. Applicant contends that the Examiner's citations to portions of the application that are not admitted prior art are evidence of improper hindsight in characterizing the Wang reference. The Examiner is not allowed to use

rationale provided by the present invention as motivation to modify or interpret the teachings of a prior art reference.

To use the applicant's own teaching to establish anticipation or obviousness is in direct contravention of cases cited by the Examiner in the final Office Action (In re Fine, 5 USPQ2d 1596 (CAFC 1988); In re Bozek, 163 USPQ 545 (CCPA 1969); In re Gershon, Goldberg, and Neiditch, 152 USPQ 602 (CCPA 1967); and In re Beattie, 24 USPQ2d 1040 (CAFC 1992)). Each of those cases mandate that the PTO must establish some objective teaching in the prior art, or knowledge generally available in the prior art, to satisfy either the all-elements rule of M.P.E.P. § 2131, or the motivation to combine references of M.P.E.P. §2143.01. The PTO has made no showing that knowledge of the above-cited clause was generally available in the prior art, and so the prima facie case for obviousness has not been met. See M.P.E.P. § 2143.

There are numerous ways in which the TP may initiate contact with a PEAD, including a continuous search by the requesting device using a known wireless protocol anytime the device is powered, or a keypad entry at the computer by a retail cashier upon a manual request by the user to utilize his/her PEAD to approve the transaction. (Applicant/Appellant does not by the above admit those ways were known prior to the date of the application.) Regardless of disclosure in the present application, Wang fails to teach or suggest a computer that automatically sends a message to a mobile station in response to receiving a message from the website that requires authentication, as recited in varying forms in each of the independent claims.

Neither Ladd nor Donoho teach or suggest a computer that automatically sends a message to a mobile station upon detecting the presence of a message from a website that requires authentication, and the Examiner does not contend that either of them do.

Claim 21 depends from claim 16 and recites that the received message be automatically detected using message parsing, for which the Examiner cites Donoho as teaching. However, no combination of Wang, Donoho, or Ladd teaches or suggests that a computer automatically detects a received message by message parsing, and in response, automatically sending a message to the mobile station.

Claims 11 and 12 that depend from claim 7, and claim 18 that depends from claim 16, each recite that the user response comprises a user authentication, a payment request, a digital signature, or any of them. However, Wang does not disclose, teach or suggest such a user response in the context of a message that is sent to the mobile station in response to detecting the presence of the message at the computer.

Applicant/Appellant therefore contends that no combination of cited references teach or suggest all claim limitations in any of the pending independent claims, as required under M.P.E.P. § 2143.03, and that all claims are patentable for at least that reason.

Issue B: Does the Wang reference anticipate a list of certificates as recited in each of claims 23-25 and 28-31?

M.P.E.P. § 2131 (and cases cited therein) require that a prior art reference must describe, either expressly or inherently, each and every element recited in a claim in order to render the claim anticipated.

Each of claims 23, 30, and 31 are independent claims that recite, in similar but not identical language, a list of certificates that are applicable to the website request and accessible by the mobile station. Examples of such certificates are recited in the written description at page 15, line 16 through page 16, line 14, and include private cryptography keys and/or digital signatures that may be stored within a secure electronic transaction (SET) wallet 27A, a smartcard 30, or an authentication module 13A of the mobile station 10. A portion of claim 23 is presented below as illustrative of the relevant claim language:

> in response to automatically detecting the presence of the received request, sending an inquiry to the mobile station from the computer for *a list of certificates that are applicable to the request*, the certificates being accessible by the mobile station;
>
> *presenting the list of applicable certificates* to the user for selecting one of the presented certificates; (emphasis added)

Claim 31 recites nearly identical language, and claim 31 recites "a list of mobile station accessible certificates that are applicable to the request,". Claim 29 recites that the list of certificates is displayed to the user using the computer interface or a mobile station interface.

As noted above, Wang is directed to a method and portable electronic authorization device (PEAD) for authorizing electronic transactions. The methods of Wang include receiving an executable portion of a program at a computer or ATM, using the executable portion to search for the PEAD, approving the transaction at the PEAD, and transmitting the approval from the PEAD. See Wang, col. 3, lines 8-20, 24-35 and 39-55.

Applicant/Appellant contends that Wang does not disclose or anticipate a list of certificates from which a user may select. In one embodiment, the PEAD includes a screen for a user to review a proposed transaction (col. 5, lines 15-18, #610 of Figure 6A) and a switch 210 to approve the transaction (col. 5, lines 19-24, Figures 2, 3A and 4). In another embodiment, there is an approve button 606 and a skip button 608 by which a user can accept or decline a proposed transaction (col. 11, lines 47-53, Figures 6A-6B). No embodiment anticipates that the user may select from several certificates, and Wang appears to teach away from such a modification in two respects: by the bare switch and approve/skip buttons noted above; and for security reasons that pervade the reference. Regarding the latter, Wang's disclosure regarding public-private key encryption at col. 5, lines 42-44 and 55-57 (and elsewhere) references a single private key within the PEAD. Wang's disclosure of an "electronic signature" at col. 7, lines 46-60, does not teach, suggest, or imply that a user may select between a digital signature and a private key for

completing one certificate selected from a list of disparate certificates. Wang's discussion of the transaction program (TP) does not appear to disclose either that a list of certificates may be sent from the requesting device to the PEAD, or that the PEAD present the user with a list of certificates.

Wang does not appear to disclose that a list of certificates be displayed on either a user interface of the computer or of the mobile station as recited in claim 29, which depends from claim 30.

Claim 24 recites that the request comprises a request for an authenticated certificate. Claim 24 depends from claim 23, which recites the mobile station present a list of certificates applicable to the request to a user. Implied in claim 24 then is that the list of certificates presented by the mobile station to a user is not merely a repetition of the request received at the computer, which is for one completed certificate. Wang does not disclose, teach, or imply any change in the request from the website to the PEAD, and especially no substantive change. In the context of Wang's lack of teaching regarding a list of certificates, claim 24 is contended as not anticipated.

Claim 25 depends from claim 23 and recites that the applicable certificates comprise signature certificates. Wang does not anticipate, teach or suggest a plurality of any kind of certificate at any stage in a transaction process.

Claims 26-27 depend from claim 23, and recite that the received request is detected based on message parsing and multi-purpose internet mail extensions (MIME) field recognition,

respectively. The Examiner cites Donoho as teaching message parsing and MIME field recognition, but no combination of Wang, Ladd, and Donoho teach or suggest detecting the message using message parsing and presenting a list of certificates to the user.

Applicant/Appellant contends that Wang fails to disclose or anticipate a list of certificates, applicable to a request from a website, that are sent from a computer to a mobile station as recited substantially in each of claims 23 and 30-31, and that those claims are patentable for at least that reason.

Issue C: Can the Wang reference be modified to make obvious that a user authentication message or user personal identification is passed outside a mobile station as recited in claims 1, 10 and 28?

Prior art references must be considered as a whole, including disclosures that teach away from the claims. M.P.E.P. § 2141.02. Proposed modifications to a prior art reference cannot render the reference unsatisfactory for its intended purpose, or change its principle of operation. M.P.E.P. § 2143.01.

Claim 1 recites, in relevant part:

> in response to receiving the message over the link, generating a user authentication message that is generated by prompting the user to enter a personal identification number (PIN) and comparing the entered PIN to a PIN stored in the mobile station;

passing the user authentication message from the mobile station to the computer over the bi-directional transmission link; (emphasis added)

Claim 10 depends from claim 7 and recites that a user response comprise user authentication. Claim 28 recites that the user personal identification information is verified in cooperation with the source of the selected certificate. Since claim 28 depends from claim 23, which recites that the mobile station communicates with a source of the selected certificate, the source used to verify the personal identification information in claim 28 is necessarily not within the mobile station.

As above, Wang is directed to a method and portable electronic authorization device (PEAD) for authorizing electronic transactions. The methods of Wang include receiving an executable portion of a program at a computer or ATM, using the executable portion to search for the PEAD, approving the transaction at the PEAD, and transmitting the approval from the PEAD. See Wang, col. 3, lines 8-20, 24-35 and 39-55.

Wang distinguishes between transaction approval (authorization) and user authentication (identification). Wang discloses at col. 11, line 61 to col. 12, line 2, an optional user authentication mechanism 612 that may be used to prevent unauthorized use of the PEAD by requiring entry of a password, fingerprint, biometrics, or other identifying characteristic *before* the proposed transaction can be approved by the PEAD. Clearly, an unauthorized user may use the PEAD to approve transactions where the optional authentication mechanism is not present. As such, Wang clearly distinguishes user authentication and

identification, which is optional, from transaction approval, which is indispensable to the Wang invention.

In the terminology of Wang at col. 4, lines 56-61 and col. 5, lines 38-39, the requesting device 202 is an ATM, computer, network, etc. that permits a user to transact business with an electronic transaction system, of which the requesting device is a part. Wang consistently and unequivocally teaches away from user authentication or personal identification (as opposed to transaction approval) being entered into the electronic transaction system. Wang recites at col. 5, lines 29-34: "The present invention is different from the prior art technique of FIG. 1 in that the user is required in the prior art to enter his *identification* information into the electronic transaction system, e.g., into ATM 100, to *authenticate* himself. In contrast, the present invention keeps the identification data related to the user secure within the PEAD 200 *at all times*." (emphasis added) Wang, col. 6, lines 61-64 states explicitly that the user identification data is *never* exposed (emphasis added). These surely are teaching away from transmitting user authentication (claims 1 and 10) or personal identification (claim 28) from a mobile station. (It is noted that claim 28 alternatively allows for the entry of personal identification data at the computer user interface. Since Wang explicitly teaches away from that alternative as noted immediately above, the argument below is directed only to the remaining claim 28 alternative of transmission from the mobile station, as well as to claims 1 and 10.)

Wang states again at col. 6, lines 25-28: " ... transaction approval in the prior art takes place within the electronic transaction system. In contrast, the present invention allows transaction approvals to take place within the PEAD 200.". No portion of Wang is seen to

diminish the veracity of the teaching that transaction approvals take place entirely within the PEAD for transmittal, and authentication/identification never leave the PEAD. This is the whole teaching of Wang, and to change that teaching is to change its principle of operation.

The user authentication recited in claims 1 and 10 above, and the personal identification data of claim 28, are by their plain language an authentication or identification of the user, and not an approval itself of the transaction. Such approval, if granted, takes place within the computer-website portion of the communication system, which Wang characterizes as the electronic transaction system to which identification and authorization data are not exposed for security reasons.

Wang repeatedly notes security deficiencies in the prior art. At col. 1, lines 57-63, Wang recites that the prior art requires the user to manually enter identification data such as a password that is compared with previously stored data to authenticate an electronic transaction. Entering a PIN at an ATM (col. 2, lines 17-23) is not secure from unauthorized procurement for at least two reasons: another party may see the user enter the PIN at the keypad (col. 2, lines 41-44), and user identification data could be intercepted while stored for some period of time within the ATM (col. 2, lines 50-54). Wang expresses at col. 2, lines 62-66, a desire to substantially eliminate the risk of unauthorized procurement of user identification data. Transmitting user authentication to a computer as recited in claims 1 and 10, or verifying personal identification data with a source outside the mobile station as in claim 28, undermines the security of approving a transaction within the PEAD. Applicant/Appellant can contemplate no logical reason for

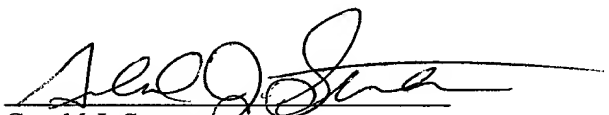
passing identification data outside a device that itself authenticates identity and approves financial transactions within it. To modify Wang such that authentication or identification of the user is transmitted from a mobile station exposes the transmitted data to unauthorized procurement for the time it is stored, directly in opposition to Wang's teachings recited above, and directly violating Wang's principle of operation that user authentication/identification never leave the PEAD.

Applicant/Appellant therefore contends that Wang cannot be so modified by any reference, and that claims 1, 10 and 28 are patentable over Wang for at least that reason.

For at least the above reasons, the Applicant/Appellant respectfully requests the Board reverse the final rejection in the Office Action of July 16, 2003, and rule that the pending claims are patentable over the cited art.

Respectfully submitted:

HARRINGTON & SMITH, LLP



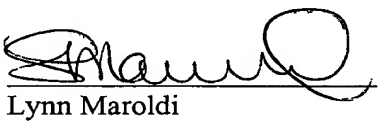
Gerald J. Stanton
Reg. No.: 46,008

October 14, 2003
Date

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

October 14, 2003
Date



Lynn Maroldi

(9) APPENDIX

Listing of Claims:

1. (Previously Presented) A method for conducting electronic commerce, comprising steps of:

operating a computer to contact a commerce-related site using a browser;

automatically detecting a presence of a message received from the commerce-related site that requires, as a response, non-stored authentication information inputted by a user in response to the detected presence of the message;

in response to automatically detecting the presence of the message, sending a message from the computer to a mobile station over a bi-directional transmission link;

in response to receiving the message over the link, generating a user authentication message that is generated by prompting the user-to-enter a personal identification number (PIN) and comparing the entered PIN to a PIN stored in the mobile station;

passing the user authentication message from the mobile station to the computer over the bi-directional transmission link; and

sending user authentication information from the computer to the commerce-related site using the browser.

2. (Canceled)

3. (Original) A method as in claim 1, wherein the user authentication message is comprised of at least one of a cryptogram and a digital signature.

4. (Original) A method as in claim 1, wherein the steps of detecting a presence of the received message and sending the message from the computer to the mobile station include a step of operating a browser plug-in software module.

5. (Previously Presented) A method as in claim 1, wherein the steps of automatically detecting a presence of the received message and sending the message from the computer to the mobile station include a step of operating a browser module.

6. (Original) A method as in claim 1, wherein the link is implemented using Bluetooth technology.

7. (Previously Presented) A system for conducting communication with a site reachable through a data communications network, comprising:

a mobile station comprising a user interface and a mobile station utilization application; and

a computer coupled to a data communications network and comprising a browser for contacting the site through the data communications network, the computer and browser operating to automatically detect a presence of a received message from the site that requires a response from the user, and further comprising an interface for sending a message from the computer to the mobile station over a bi-directional link in response to automatically detecting the presence of the message;

said mobile station utilization application being responsive to the receipt of the message from the link for generating a user response message and for passing the user response message to the computer over the link, said mobile station operating to prompt the user to enter a personal identification number (PIN) into the mobile station and to compare the entered PIN to a PIN stored in the mobile station; and

said computer being responsive to a receipt of said user response message for sending user response information to the site using said browser.

8. (Canceled)

9. (Previously Presented) A system for conducting communication with a site reachable through a data communications network, comprising:

a mobile station comprising a user interface and a mobile station utilization application; and

a computer coupled to a data communications network and comprising a browser for contacting the site through the data communications network, the computer and browser operating to automatically detect a presence of a received message from the site that requires a response from the user, and further comprising an interface for sending a message from the computer to the mobile station over a bidirectional link in response to automatically detecting the presence of the message;

said mobile station utilization application being responsive to the receipt of the message from the link for generating a user response message and for passing the user response message to the computer over the link; and

said computer being responsive to a receipt of said user response message for sending user response information to the site using said browser,

wherein said computer operates to prompt the user to enter a personal identification number (PIN) into said computer, said computer transmits the entered PIN to said mobile station over the link, and where a user authentication module in said mobile station compares the entered PIN to a PIN stored in the mobile station.

10. (Original) A system as in claim 7, wherein said user response is comprised of a user authentication.

11. (Original) A system as in claim 7, wherein said user response is comprised of a payment request.

12. (Original) A system as in claim 7, wherein said user response is comprised of a digital signature.

13. (Original) A system as in claim 7, wherein said site is comprised of a site operated by a merchant that is reached through the Internet.

14. (Original) A system as in claim 7, wherein at least one electronic ticket is downloaded from said site, via said browser, to a memory of said mobile station.

15. (Original) A system as in claim 7, wherein said link is implemented using Bluetooth technology.

16. (Previously Presented) A method for conducting communication with a site reachable through a data communications network, comprising steps of:

providing a mobile station having a user interface and an application;

coupling a computer to a data communications network, the computer having a browser for contacting the site through the data communications network;

automatically detecting with the computer a presence of a received message from the site that requires a response from the user;

in response to automatically detecting the presence of the received message, sending a message from the computer to the mobile station over a bi-directional link;

responsive to the receipt of the message in the mobile station and an input of a personal identification number (PIN) and a comparison of the inputted PIN to a PIN stored in the mobile station, generating a user response message and passing the user response message to the computer over the link; and

responsive to a receipt of the user response message in the computer, sending user response information to the site using the browser.

17. (Canceled)

18. (Original) A method as in claim 16, wherein said user response is comprised of at least one of a user authentication, a payment request, or a digital signature.

19. (Original) A method as in claim 16, wherein the site is operated by a merchant and is reached through the Internet.

20. (Original) A method as in claim 16, wherein data is downloaded from the site, via the browser, to a memory of the mobile station.

21. (Previously Presented) A method as in claim 1, where the received message is automatically detected using message parsing.

22. (Previously Presented) A method for conducting communication with a site reachable through the Internet, comprising:

providing a mobile station;

coupling a browser running on a computer to the site through the Internet;

automatically detecting a presence of a received challenge from the site, the received challenge being detected based on message parsing that comprises Multi-Purpose Internet Mail Extensions (MIME) field recognition;

in response to automatically detecting the presence of the received challenge, sending at least one message from the computer to the mobile station over a bidirectional wireless link;

responsive to the receipt of the at least one message in the mobile station, generating a response to the challenge and transmitting the response to the computer over the link, where generating the response comprises prompting the user to enter personal

identification information using one of a computer user interface or a mobile station user interface, and operating a user authentication module in the mobile station to validate the entered personal identification information; and

responsive to a receipt of the response at the computer, sending a response to the challenge to the site using the browser.

23. (Previously Presented) A method for conducting communication with a site reachable through the Internet, comprising:

providing a mobile station;

coupling a browser running on a computer to the site through the Internet;

automatically detecting a presence of a received request from the site;

in response to automatically detecting the presence of the received request, sending an inquiry to the mobile station from the computer for a list of certificates that are applicable to the request, the certificates being accessible by the mobile station;

presenting the list of applicable certificates to the user for selecting one of the presented certificates;

using the mobile station to communicate with a source of the selected certificate for completing the certificate;

passing the completed certificate to the browser; and

responsive to a receipt of the completed certificate, responding to the request received from the site.

24. (Previously Presented) A method as in claim 23, where the request comprises a request for an authenticated certificate, where the applicable certificates comprise authentication certificates, and where the completed certificate comprises an authenticated certificate.

25. (Previously Presented) A method as in claim 23, where the request comprises a request for a digital signature, where the applicable certificates comprise signature certificates, and where the completed certificate comprises a signed signature certificate.

26. (Previously Presented) A method as in claim 23, where the received request is detected based on message parsing.

27. (Previously Presented) A method as in claim 26, where message parsing comprises Multi-Purpose Internet Mail Extensions (MIME) field recognition.

28. (Previously Presented) A method as in claim 23, where completing the certificate comprises prompting the user to enter personal identification information using one of a computer user interface or a mobile station user interface, and verifying the entered personal identification information in cooperation with the source of the selected certificate.

29. (Previously Presented) A method as in claim 23, where the list of applicable certificates are displayed to the user using one of a computer user interface or a mobile station user interface.

30. (Previously Presented) A mobile station for conducting communication with a server reachable through a data communications network, comprising:

a bidirectional data path for coupling to a network access application; and

a controller, responsive to an automatic detection of a presence of a received request from the server by the access application or an extension of the access application, and to a reception of an inquiry from the access application, or the extension of the access application, for a list of mobile station accessible certificates that are applicable to the request, for returning the list of applicable certificates, and in response to the user selecting one of the certificates, for communicating with a source of the selected certificate for completing the certificate and passing the completed certificate to the network access application for responding to the request received from the server.

31. (Previously Presented) A method for conducting communication with a server, comprising:

coupling an access application running on a computer to the server through a data communications network;

automatically detecting a presence of a request that is received from the server, the request being one that requires an authentication of a user;

in response to automatically detecting the presence of the request, sending a message from the computer to a mobile station over a link; the message comprising an inquiry for a list of certificates that are applicable to the request, the certificates being accessible by the mobile station;

presenting the list of applicable certificates to the user for selecting one of the presented certificates;

using the mobile station to communicate with a source of the selected certificate for completing the certificate which comprises a user authentication message;

passing the completed certificate over a link to the access application running on the computer;

responsive to a receipt of the completed certificate, sending user authentication information to the server using the access application.

32. (Canceled)